RMF

Cybersecurity and the Risk Management Framework

Where we've been and where we're going

~~Information Assurance~~

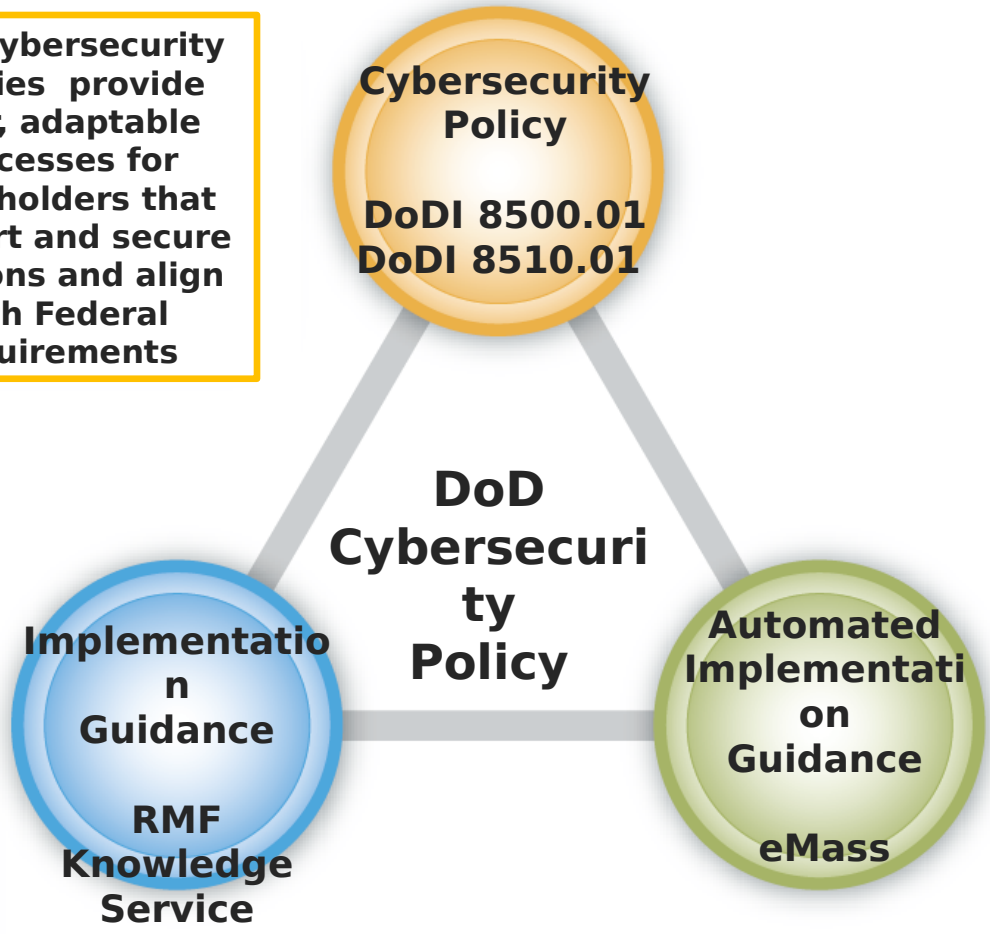
DoD Instruction 8500.01, Para 1(d), adopts the term "cybersecurity" as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 to be used throughout the DoD instead of the term "information assurance (IA)."

Cybersecurity Defined

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

DoD Cybersecurity Policy and the RMF

DoD Cybersecurity Policies provide clear, adaptable processes for stakeholders that support and secure missions and align with Federal requirements



The RMF Knowledge Service is the authoritative source for information, guidance, procedures, and templates on how to execute the Risk Management Framework

Automated Tools such as the Enterprise Mission Assurance Support Service (eMASS) and the Ports, Protocols, and Services Management (PPSM) registry enable agile deployment

Cybersecurity Policy Update

DoDI 8500.01 “Cybersecurity”

- Extends applicability to all IT processing DoD information,
- Emphasizes operational resilience, integration, and interoperability
- Aligns with Joint Task Force Transformation Initiative (DoD, NIST, IC, and CNSS)
- Transitions to the newly revised NIST SP 800-53 Security Control Catalog
- Adopts common Federal cybersecurity terminology so we are all speaking the same language
- Leverages and builds upon numerous existing Federal policies and standards so there is less DoD policy to write and maintain
- Incorporates security early and continuously within the acquisition lifecycle
- Facilitates multinational information

DoDI 8510.01 “Risk Management Framework (RMF) for DoD Information Technology (IT)”

- Adopts NIST’s Risk Management Framework
- Clarifies what IT should undergo the RMF process
- Strengthens and supports enterprise-wide IT governance and authorization of IT systems and services
- Moves from a checklists to a risk based approach
- RMF steps and activities are embedded in DoD Acquisition Lifecycle
- Promotes DT&E and OT&E integration
- Implements cybersecurity via security controls vice numerous policies and memos
- Adopts reciprocity and codifies reciprocity tenets
- Emphasizes continuous monitoring and timely correction of deficiencies

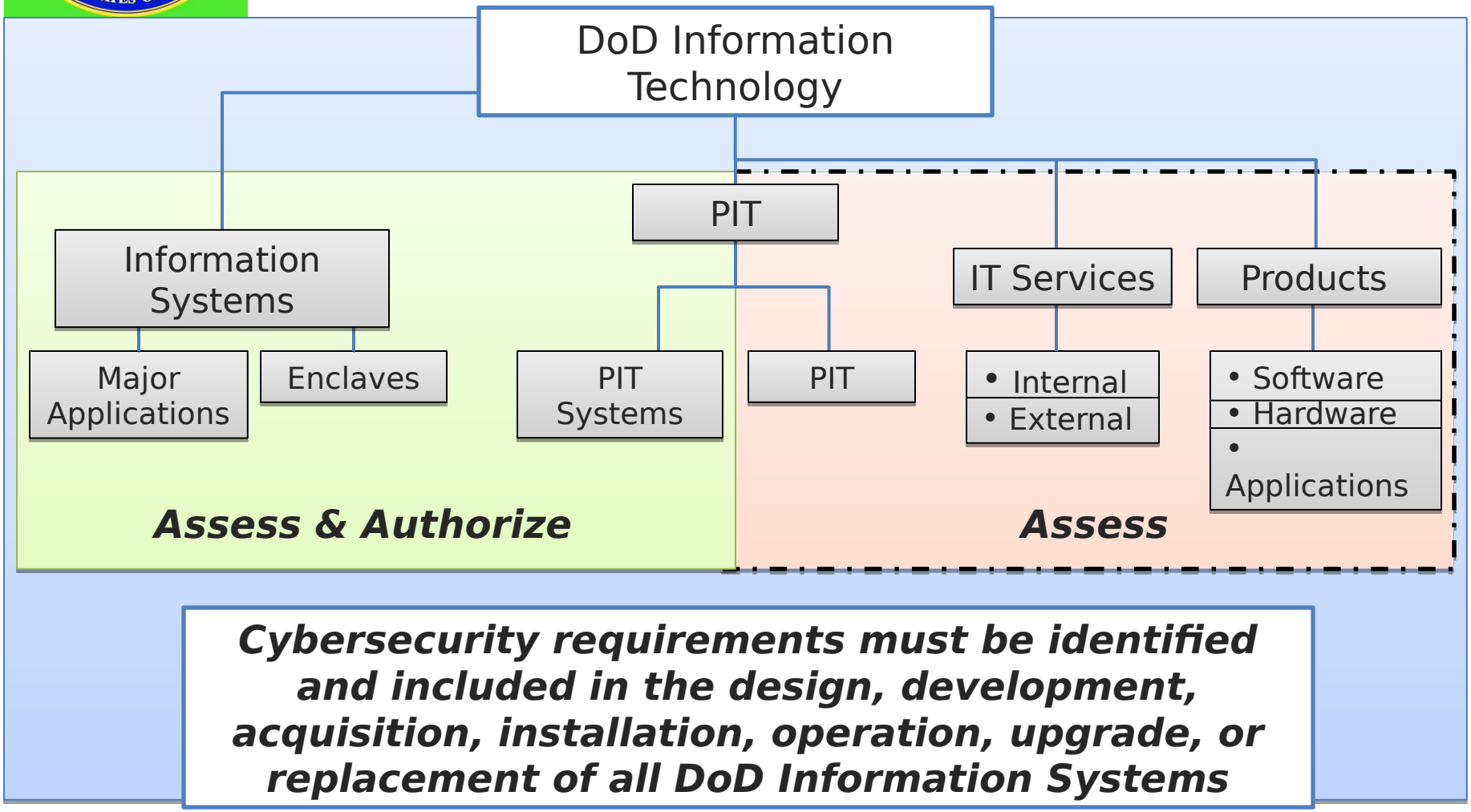
Cybersecurity Applicability

All DoD-owned IT or DoD-controlled IT that receives, processes, stores, displays, or transmits DoD information

- All DoD information in electronic format
- Special Access Program (SAP) information technology, other than SAP IS handling sensitive compartmented information (SCI)
- IT supporting research, development, test and evaluation (T&E), and DoD-controlled IT operated by a contractor or other entity on behalf of the DoD

DoD information technology (IT) is broadly grouped as DoD information systems (ISs), platform IT (PIT), IT services, and products

DoD Information Technology



Cybersecurity requirements must be identified and included in the design, development, acquisition, installation, operation, upgrade, or replacement of all DoD Information Systems

Cybersecurity Applicability

Managing cybersecurity risks is complex and requires the involvement of the entire organization including

- Senior leaders planning and managing DoD operations
- Developers, implementers, and operators of IT supporting operations

Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions and includes

- Cost, performance, and schedule risk for programs of record
- All other acquisitions of the DoD

The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources

Cybersecurity Risk Management Roles

DoD Chief Information Officer (CIO)

- Coordinates with Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) to ensure that cybersecurity is integrated into processes for DoD acquisition programs, including research and development
- Coordinates with the Director of Operational Test and Evaluation (DOT&E) to ensure that cybersecurity responsibilities are integrated into the operational testing and evaluation for DoD acquisition programs

USD(AT&L)

- Integrates cybersecurity policies and supporting guidance into acquisition policy, regulations, and guidance
- Ensures the DoD acquisition process incorporates cybersecurity planning, implementation, testing, and evaluation
- Ensures acquisition community personnel with IT responsibilities are qualified

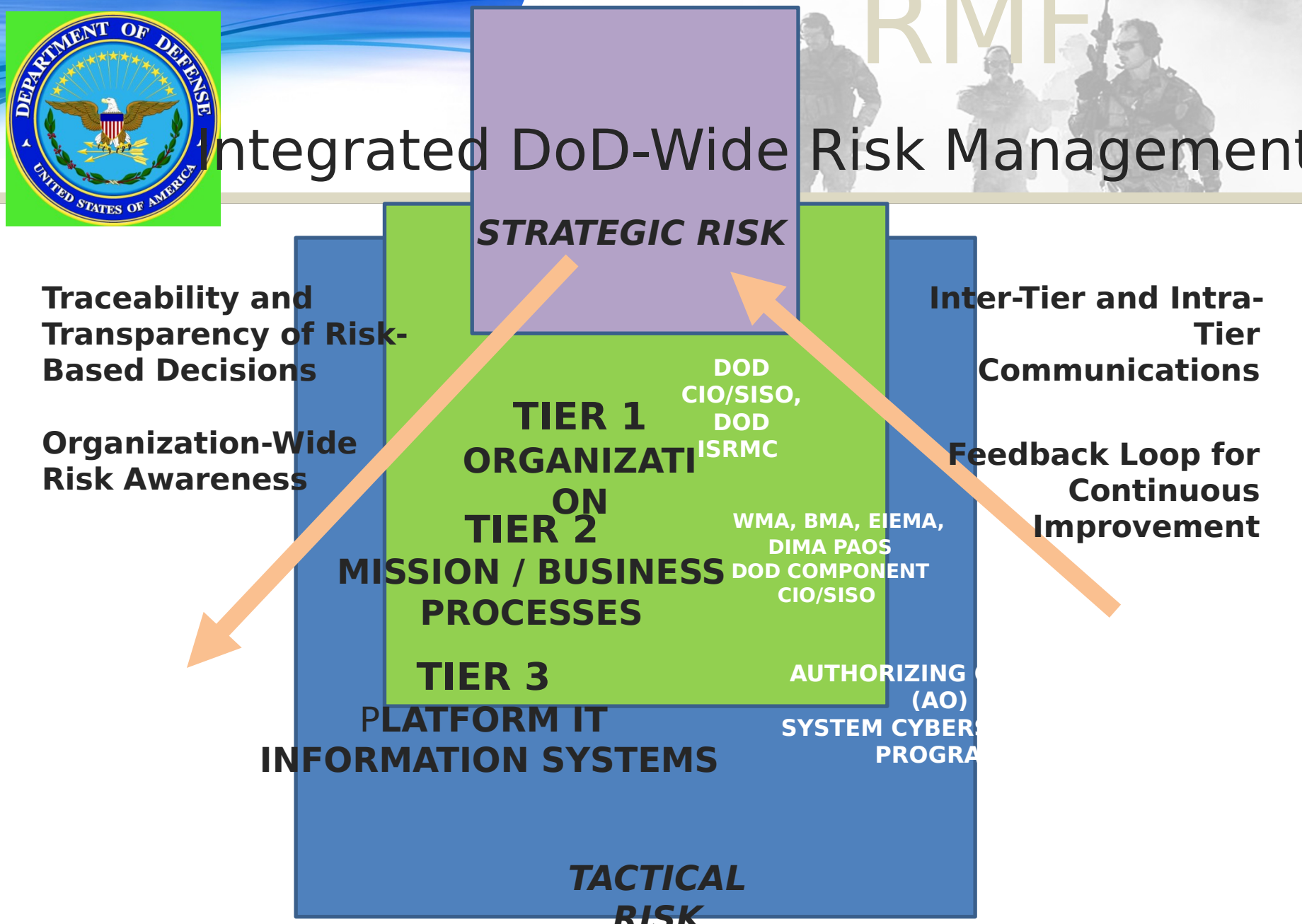
DoD Component Heads

- Ensure system security engineering and trusted systems and networks processes, tools and techniques are used in the acquisition of all applicable IT

RMF Promotes DT&E and OT&E Integration

DoD CIO, in coordination with the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation DASD(DT&E) and DOT&E, ensures developmental and operational test and evaluation activities and findings are integrated into the RMF

Integrated DoD-Wide Risk Management



Tier 1 Risk Management Roles

DoD CIO (Chief Information Officer) develops and establishes DoD Cybersecurity policy and guidance consistent with applicable statute or Federal regulations

SISO (Senior Information Security Officer) directs and coordinates the Defense Cybersecurity Program and, as delegated, carries out the DoD CIO's responsibilities

DoD RISK EXECUTIVE FUNCTION (Defined in National Institute of Standards and Technology (NIST) Special Publication 800-37) is performed by the DoD Information Security Risk Management Committee (DoD ISRMC)

Tier 2 Risk Management Roles

DoD Principle Authorizing Official (PAO) assigned for each DoD Mission Areas (MA)

- Warfighter
- Business
- Enterprise Information Environment
- Defense Intelligence

Component

- Chief Information Officer (CIO)
- Senior Information Security Officer (SISO)

Tier 3 Risk Management Roles

System Cybersecurity Program

- Authorizing Official (AO)
- Information System Owners (ISO) of DoD IT
- Information Owner (IO)
- Information System Security Manager (ISSM)
- Information System Security Officer (ISSO)

Operational Cybersecurity

Operational Resilience

- Information resources are trustworthy
- Missions are ready for information resources degradation or loss
- Network operations have the means to prevail in the face of adverse events

Operational Integration

- Cybersecurity must be fully integrated into system life cycles and is a visible element of organizational, joint, and DoD Component IT portfolios

Interoperability

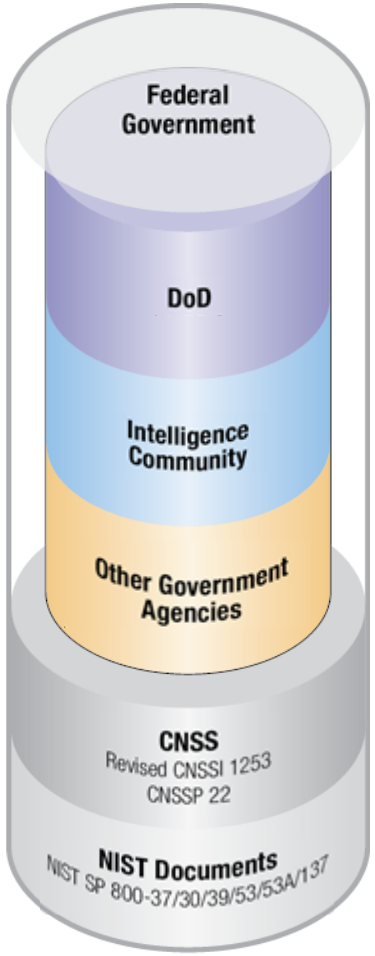
- Adherence to DoD architecture principles
- Utilizing a standards-based approach
- Manage the risk inherent in interconnecting systems

Aligning Cybersecurity Policy

Before

Joint Task Force Transformation Initiative

DoD aligns cybersecurity and risk management policies, procedures, and guidance with Joint Transformation NIST documents, the basis for a **unified information security framework for the Federal government.**

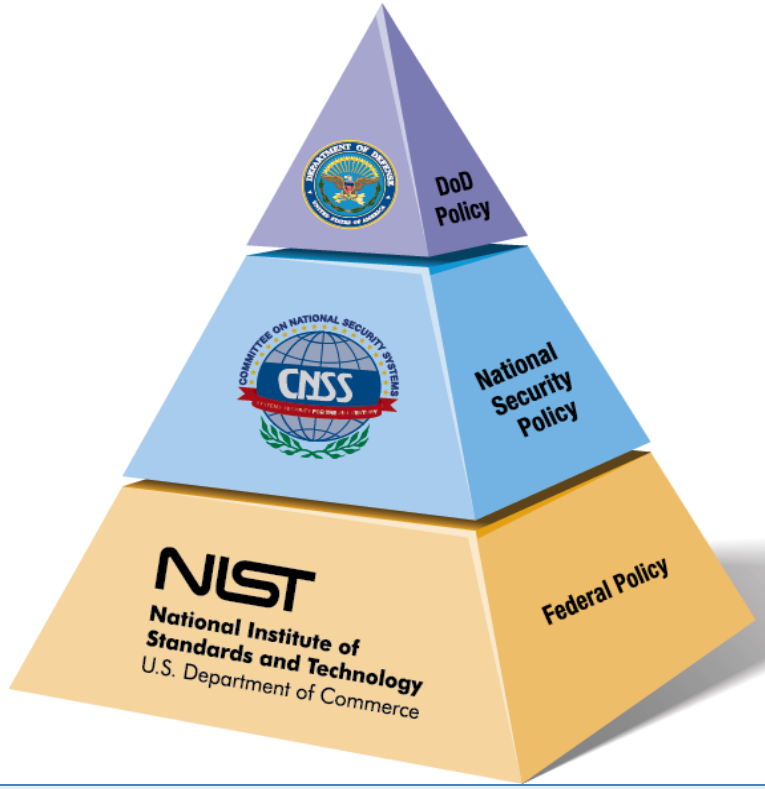


After

UNCLASSIFIED

Cybersecurity Policy Partnerships

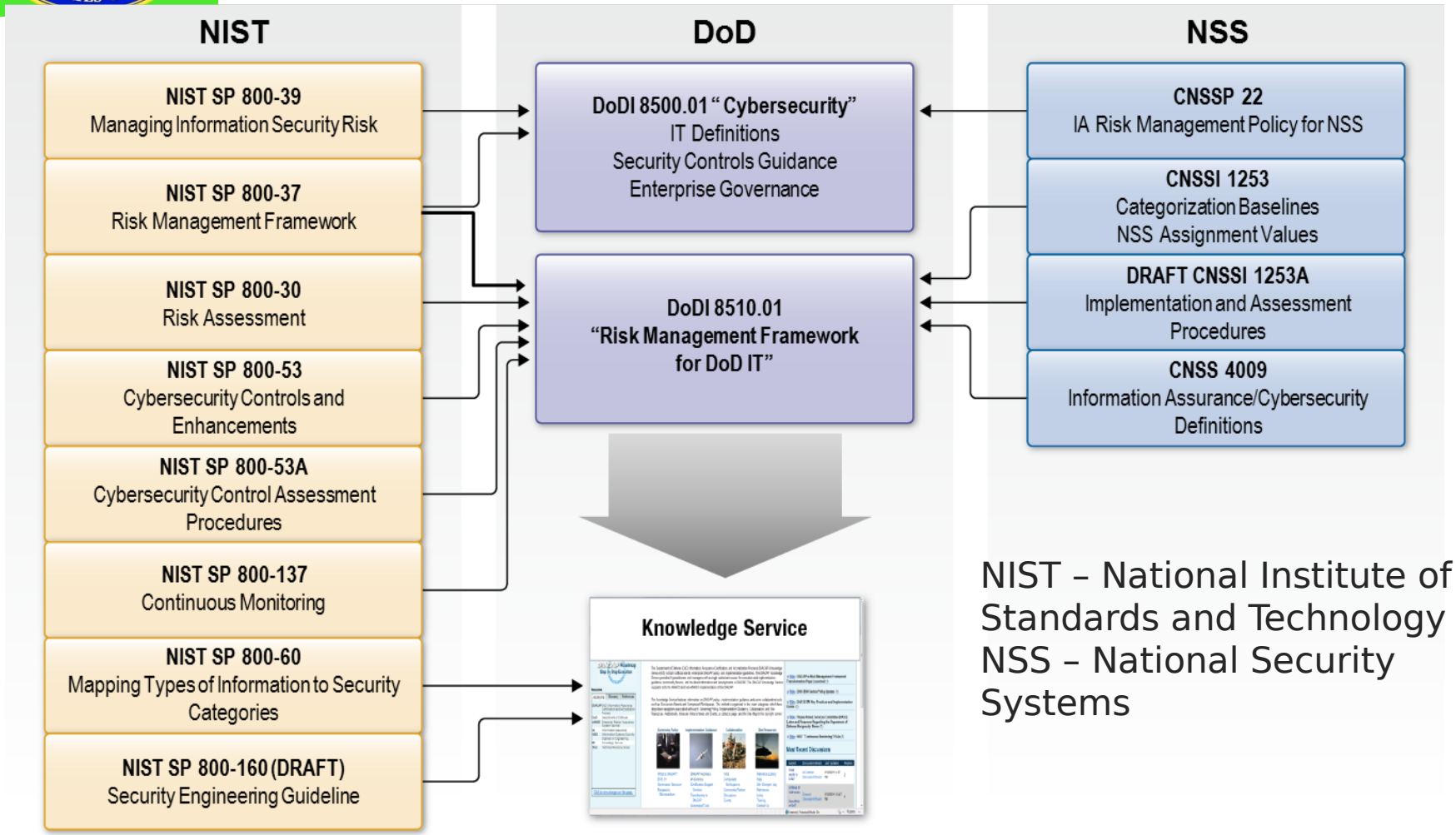
DoD participates in development of CNSS and NIST documents ensuring DoD equities are met



DoD leverages CNSS and NIST policies and filters requirements to meet DoD needs

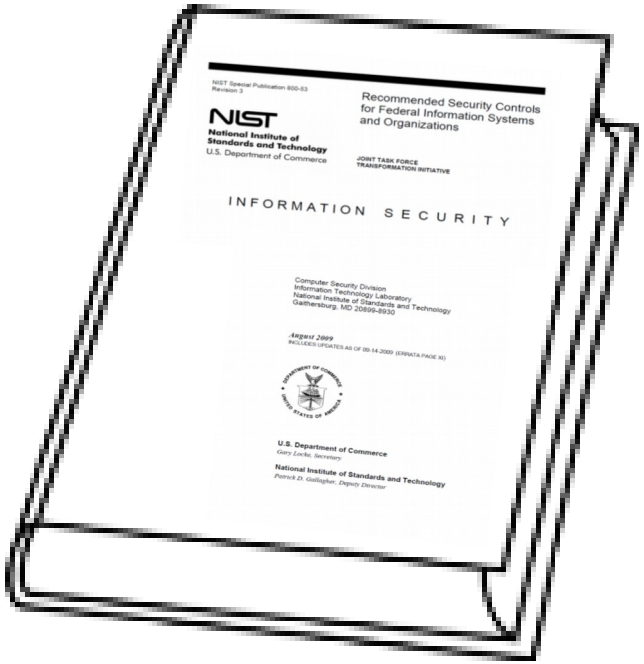
DoD participates in CNSS and NIST policy development as a vested stakeholder with the goals of a more standardized approach to cybersecurity and to protect the unique requirements of DoD missions and warfighters

Alignment Documents and Guidance



NIST – National Institute of Standards and Technology
NSS – National Security Systems

Security Control Catalog (NIST SP 800-53)

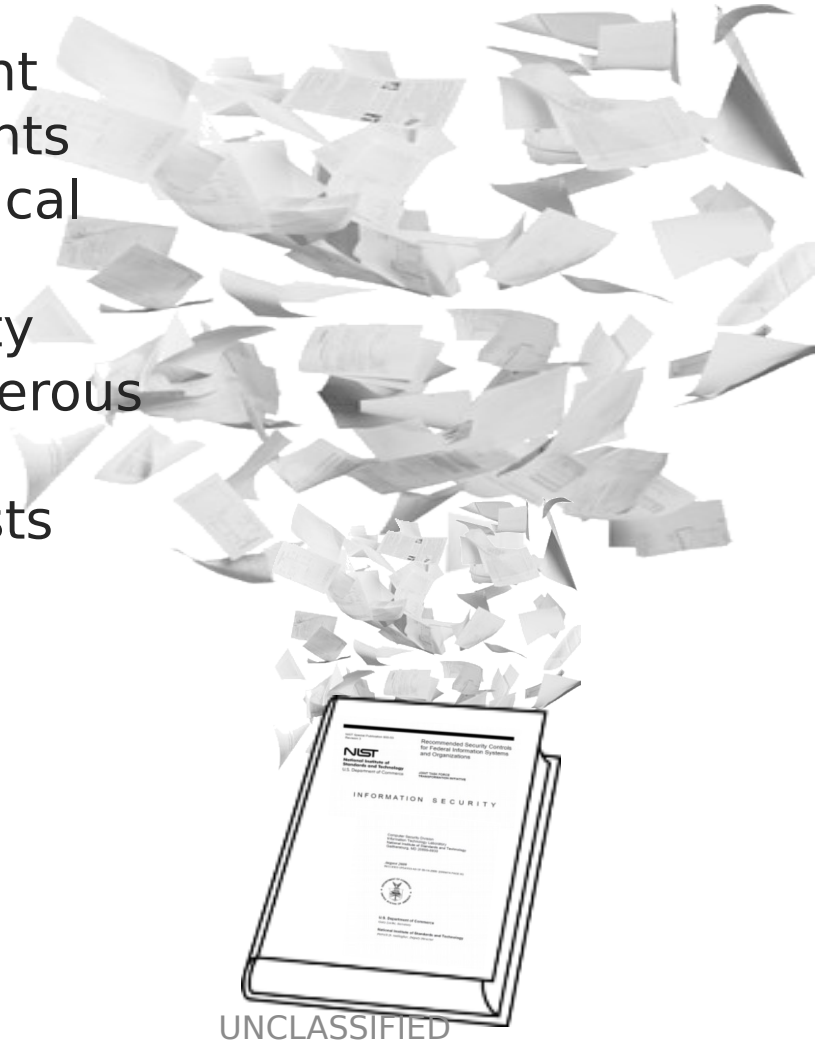

NIST Special Publication 800-53
Revision 3
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Recommended Security Controls for Federal Information Systems and Organizations
JOINT TASK FORCE TRANSFORMATION INITIATIVE
INFORMATION SECURITY
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930
August 2009
U.S. Department of Commerce
Gary Locke, Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

AC-1	Access Control Policy and Procedure
AC-2	Account Management
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AU-1	Audit and Accountability Policy and Procedures
AU-2	Auditable Events
CA-1	Security Assessment and Authorization Policy and Procedures
CM-1	Configuration Management Policy and Procedures

- Risk Management Framework (RMF) provides a built-in compliance process
  - RMF is integrated into the DoD acquisition process, which enables policy enforcement

Implementing Cybersecurity Policies

The Risk Management Framework implements cybersecurity technical policies through the application of security controls, not by numerous standalone policies, memos, and checklists



Moving to the Risk Management Framework

DIACAP Compliance Check

Are you compliant with these controls?

- ☐ Yes
- ☑ No

What is the vulnerability level (Severity Category/code) ?

- ☑ CAT I Finding

Risk Management Framework

Are you compliant with these controls?

- ☐ Yes
- ☑ No

What is the Risk?

- ☑ Vulnerability level (includes STIG findings)
- ☑ Associated Threats
- ☑ Likelihood of Exploitation
- ☑ Impact level (CIA)
- ☑ Compensating Controls and Mitigations

What is the Residual Risk? What is my organization's risk tolerance? What is my risk tolerance?

- ☑ Risk Accepted

DoD RMF Process Adopts NISTs RMF

RMF

Enterprise-wide Authorization ISs & Services

Common Control

- Security control that is inherited by one or more organizational information systems

Security Control Inheritance

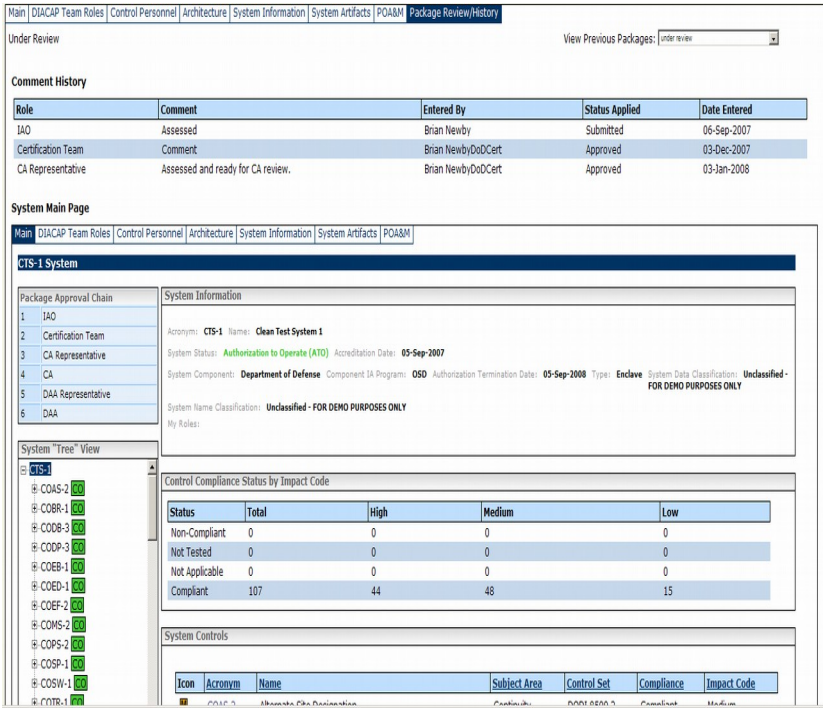
- Information system or application receives protection from security controls (or portions of security controls) that are developed, authorized, and monitored by another organization, either internal or external, to the organization where the system or application resides

Of the 900+ controls and enhancements in the NIST SP 800-53 Rev. 4 Catalog, about 400 typically apply to an IS. Of the 400, many are "common controls" inherited from the hosting environment; this is great use of the "build once/use many" approach.

RMF Encourages Use of Automated Tools

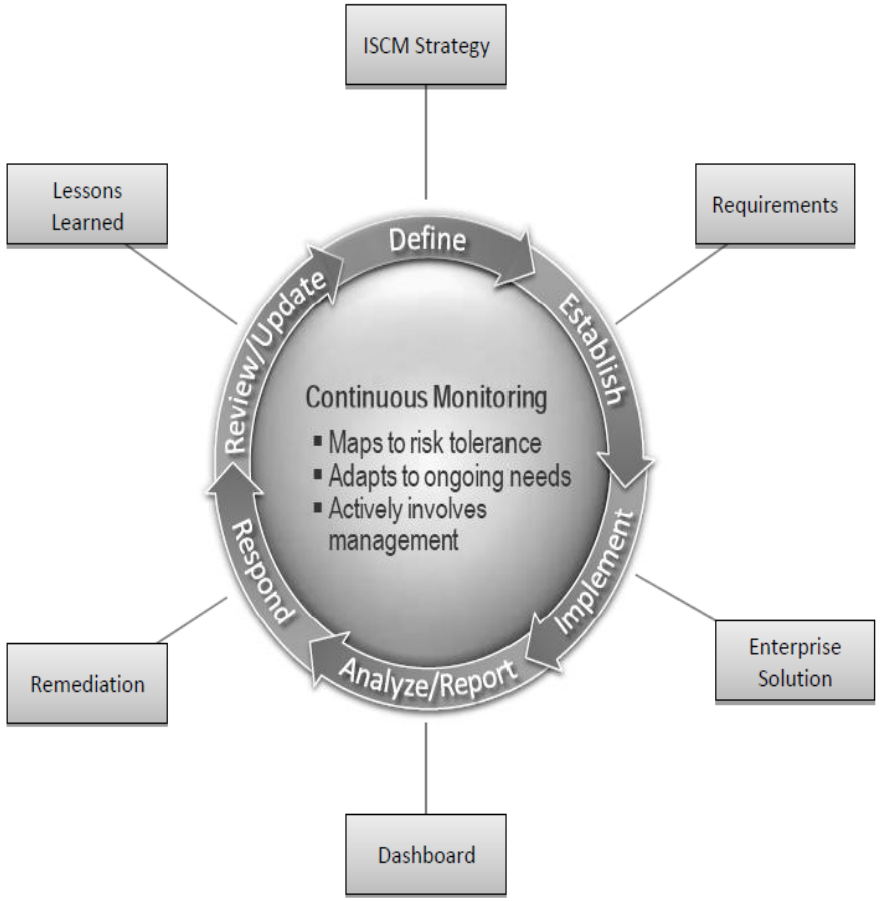
Some security controls, baselines, Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), Control Correlation Identifiers (CCIs), implementation and assessment procedures, overlays, common controls, etc., *may possibly* be automated

- Automated systems are being developed to manage the RMF workflow process, to identify key decision points, and to generate control lists needed in RMF implementation
- An example of such an automated system is the DoD-sponsored Enterprise Mission Assurance Support Service (eMASS)


Main DIACAP Team Roles Control Personnel Architecture System Information System Artifacts POA&M Package Review/History
Under Review
View Previous Packages:
Comment History
Role Comment Entered By Status Applied Date Entered
IAO Assessed Brian Newby Submitted 06-Sep-2007
Certification Team Comment Brian NewbyDoDCert Approved 03-Dec-2007
CA Representative Assessed and ready for CA review. Brian NewbyDoDCert Approved 03-Jan-2008
System Main Page
Main DIACAP Team Roles Control Personnel Architecture System Information System Artifacts POA&M
CTS-1 System
Package Approval Chain
1 IAO
2 Certification Team
3 CA Representative
4 CA
5 DAA Representative
6 DAA
System Information
Acronym: CTS-1 Name: Clean Test System 1
System Status: Authorization to Operate (ATO) Accreditation Date: 05-Sep-2007
System Component: Department of Defense Component IA Program: OSD Authorization Termination Date: 05-Sep-2008 Type: Enclave System Data Classification: Unclassified - FOR DEMO PURPOSES ONLY
System Name Classification: Unclassified - FOR DEMO PURPOSES ONLY
My Roles:
System "Tree" View
CTS-1
COAS-2 CO
COBR-1 CO
CODB-3 CO
CODP-3 CO
COEB-1 CO
COED-1 CO
COEF-2 CO
COMS-2 CO
COPS-2 CO
COSP-1 CO
COSW-1 CO
Control Compliance Status by Impact Code
Status Total High Medium Low
Non-Compliant 0 0 0 0
Not Tested 0 0 0 0
Not Applicable 0 0 0 0
Compliant 107 44 48 15
System Controls
Icon Acronym Name Subject Area Control Set Compliance Impact Code

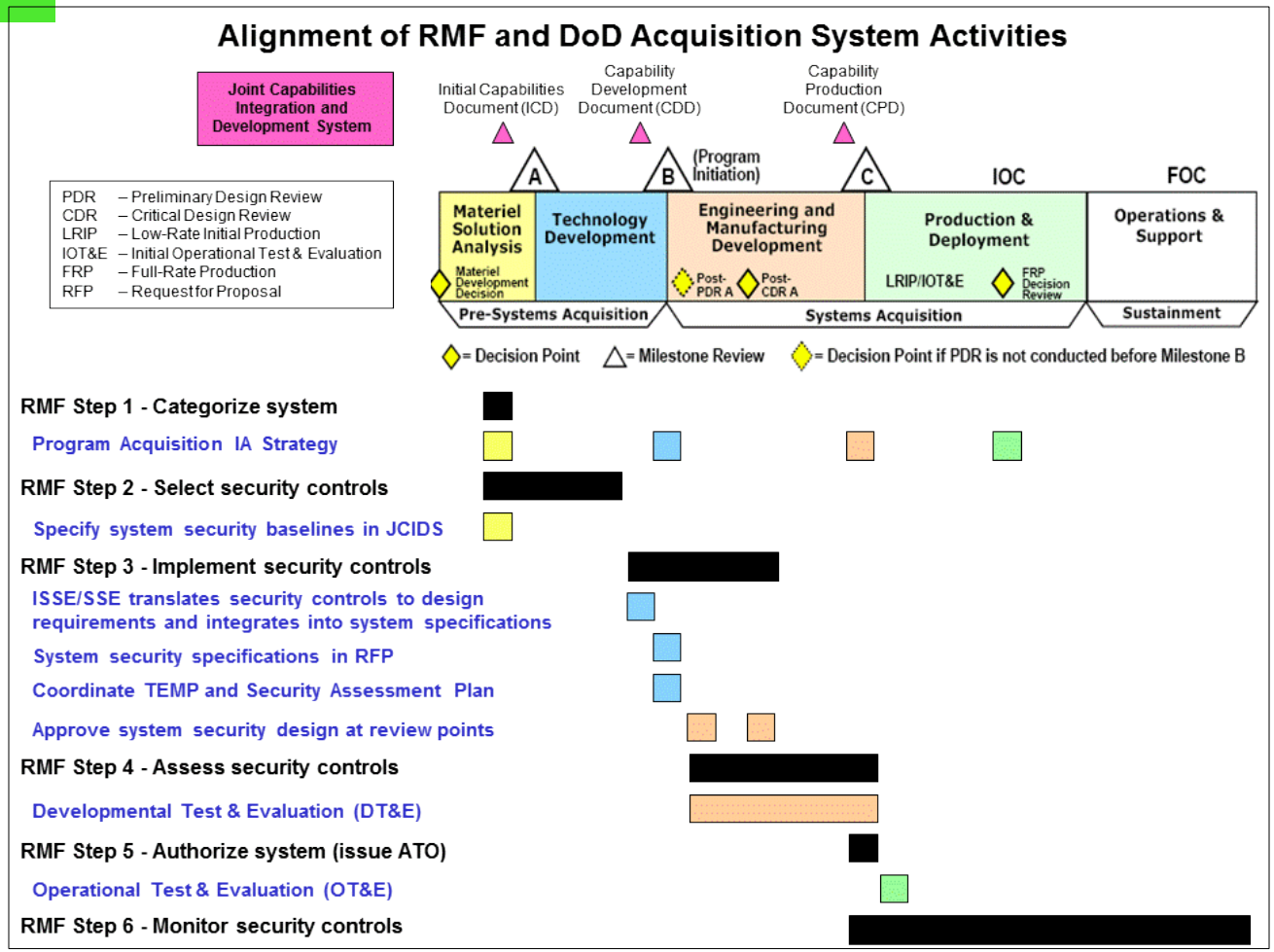
RMF Promotes ISCM

RMF sets the baseline for the initial IS authorization. Developing ongoing authorization may be accomplished by leveraging an Information Security Continuous Monitoring (ISCM) Program, with joint processes to adopt reciprocity for cybersecurity across DoD, the Intelligence Community, and Federal Agencies.



RMF Built into DoD Acquisition Lifecycle

Alignment of RMF and DoD Acquisition System Activities


Joint Capabilities Integration and Development System
Initial Capabilities Document (ICD)
Capability Development Document (CDD)
Capability Production Document (CPD)
(Program Initiation)
A
B
C
IOC
FOC
PDR – Preliminary Design Review
CDR – Critical Design Review
LRIP – Low-Rate Initial Production
IOT&E – Initial Operational Test & Evaluation
FRP – Full-Rate Production
RFP – Request for Proposal
Materiel Solution Analysis
Materiel Development Decision
Technology Development
Engineering and Manufacturing Development
Post-PDR A
Post-CDR A
Production & Deployment
LRIP/IOT&E
FRP Decision Review
Operations & Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment
= Decision Point
= Milestone Review
= Decision Point if PDR is not conducted before Milestone B
RMF Step 1 - Categorize system
Program Acquisition IA Strategy
RMF Step 2 - Select security controls
Specify system security baselines in JCIDS
RMF Step 3 - Implement security controls
ISSE/SSE translates security controls to design requirements and integrates into system specifications
System security specifications in RFP
Coordinate TEMP and Security Assessment Plan
Approve system security design at review points
RMF Step 4 - Assess security controls
Developmental Test & Evaluation (DT&E)
RMF Step 5 - Authorize system (issue ATO)
Operational Test & Evaluation (OT&E)
RMF Step 6 - Monitor security controls

Questions